ABSTRACT

The present invention relates to digital signature operations using public key schemes in a secure communications system and in particular for use with processors having limited computing power such as 'smart cards'. This invention describes a method for creating and authenticating a digital signature comprising the steps of selecting a first session parameter k and generating a first short term public key derived from the session parameter k, computing a first signature component r derived from a first mathematical function using the short term public key, selecting a second session parameter t and computing a second signature component s derived from a second mathematical function using the second session parameter t and without using an inverse operation, computing a third signature component using the first and second session parameters and sending the signature components (s, r, c) as a masked digital signature to a receiver computer system. In the receiver computer system computing a recovered second signature component s' by combining a third signature component with the second signature component to derive signature components (s', r) as an unmasked digital signature. Verifying these signature components as in a usual ElGamal or ECDSA type signature verification.